



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/621,731	07/17/2003	Kyle Nathan Patrick	CA920020058US1	1585

7590 01/12/2007
IBM Corporation
Intellectual Property Law
Dept. 1Q0A/Bldg. 040-3
1701 North Street
Endicott, NY 13760

EXAMINER

DINH, MINH

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 10/621,731	Applicant(s) PATRICK, KYLE NATHAN	
	Examiner Minh Dinh	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-3 and 5-21 is/are rejected.
- 7) ☒ Claim(s) 4 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 July 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>7/17/03</u> . | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-21 have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 1-3, 5-10, 12-16 and 17-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 1 is directed to a method for securely comparing a document possessed by two parties without one revealing the document it possesses to the other party. However, claim 1 does not recite the following three steps which are part of the method as described in the specification (page 3, next to last paragraph; page 4, first paragraph; Figure 2): (i) each party examining the other party's set of random data for suitability and aborting the comparison if suitability is not established wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data; (ii) after computing said first and second values, each said first and second parties sending confirmation to the other party that each said party's first and second values have been computed, and waiting for said confirmation from said other party that each

said party's first and second values have been computed before proceeding;

(iii) after one party has sent its first value to the other party, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time. Therefore, the method of claim 1 is not complete. A method that is not complete is not useful. Claims 8 and 15 are rejected on the same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

4. Claims 8-14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 8 is directed to a computer program product comprising a computer usable medium. The computer usable medium can be interpreted as a modulated carrier signal (Specification, page 5, second paragraph), which does not fall within one of the four statutory classes of 35 USC 101. Please refer to Annex IV of *Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility*, 1300 Off. Gaz. Pat. Office 142 (Nov. 22, 2005) (Patent Subject Matter Eligibility Interim Guidelines). Claims that are not specifically addressed are rejected by virtue of their dependency. Applicant is suggested to change "a computer usable medium" to "a computer storage medium".

5. Claims 15-21 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 15 is directed to an article comprising a modulated carrier signal, which does not fall within one of the four statutory classes of 35 USC 101. Claims that are not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-3, 5-10, 12-16 and 17-21 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: (i) each party examining the other party's set of random data for suitability and aborting the comparison if suitability is not established wherein said other party's random data is determined to be unsuitable if it is identical to said examining party's set of random data; (ii) after computing said first and second values, each said first and second parties sending confirmation to the other party that each said party's first and second values have been computed, and waiting for said confirmation from said other party that each said party's first and second values have been computed before proceeding; (iii) after one party has sent its first

value to the other party, aborting the comparison if the other party does not respond with its first value within a pre-determined length of time (Specification page 3, next to last paragraph; page 4, first paragraph; page 5, first paragraph; Figure 2).

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1, 5, 8, 12, 15 and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Menezes et al. ("Handbook of Applied Cryptography"). Menezes discloses a method of securely comparing first secret information, key K, in possession of a first party, party A, and second secret information, key K, in possession of a second party, party B, without revealing the contents of the first secret information to the second party or the contents of the second secret information to the first party (Section 10.3.2 (ii) Challenge-response based on (keyed) one-way functions, page 402). Secret information such as a cryptographic key possessed by a party as disclosed by Menezes can be written on a piece of paper and/or stored as a file, and,

therefore, is interpreted as a document. Regarding claims 1 and 5, which represents claims 8, 12, 15 and 19, Menezes specifically discloses: i) said first and second parties each generating its own set of random data, r_A and r_B (steps 1-2); ii) each party exchanging said set of random data and a shared hash function with the other party (steps 1-2); iii) each party computing a first value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by that party's set of random data, followed by the other party's set of random data (steps 2-3); iv) each party computing a second value consisting of the output of said shared hash function where the input to the hash function is the consecutive concatenation of the document in each said party's possession, followed by the other party's set of random data, followed by that party's set of random data ("rather than decrypting and verifying ... the computed MAC matches the received MAC value"); v) each party sending its first value to the other party and receiving the other party's first value (steps 2-3); and vi) each party comparing said other party's first value to its second value; vii) each party concluding that if the said values are the same, then the two documents are the same, but that otherwise said two documents are different ("rather than decrypting and verifying ... the computed MAC matches the received MAC value").

10. Claims 2-4, 6-7, 9-11, 13-14, 16-18 and 20-21 are not rejected over the prior art.

Allowable Subject Matter

11. Claim 4 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,681,017 to Matias et al.

U.S. Patent App. Publication No. 2001/0044895 to Hada

U.S. Patent App. Publication No. 2002/0049601 to Asokan et al.

U.S. Patent App. Publication No. 2003/0093680 to Astley et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

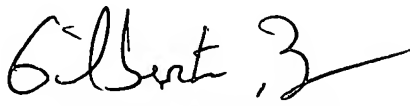
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

MD
01/02/07


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100